PREDIKCIA BEZPEČNOSTNÝCH UDALOSTÍ POUŽITÍM VIACROZMERNÝCH MODELOV ČASOVÝCH RADOV

BC. MIROSLAV VOJTEK

VEDÚCI PRÁCE: RNDR. JUDR. PAVOL SOKOL, PHD.

KONZULTANT: RNDR. ANDREJ GAJDOŠ, PHD.

DÁTA - UDALOSTI

cesnet warden

Bezpečnostné udalosti

- pôvod – WARDEN, CESNET (idea.cesnet.cz)
- 22 časových radov (počítadlá, kategórie, porty, protokoly)
- časový úsek – 1 rok

counter
counter IP-čiek
counter(iný ako 56)
recon scanning
availability DDOS
attempt login
attempt exploit
malware ransomware
intrusion botnet

21
22
23
25
80
443
445

TCP
SSH
UDP
ICMP
MSWBTSERVER
TELNET

DÁTA – ZRANITEĽNOSTI

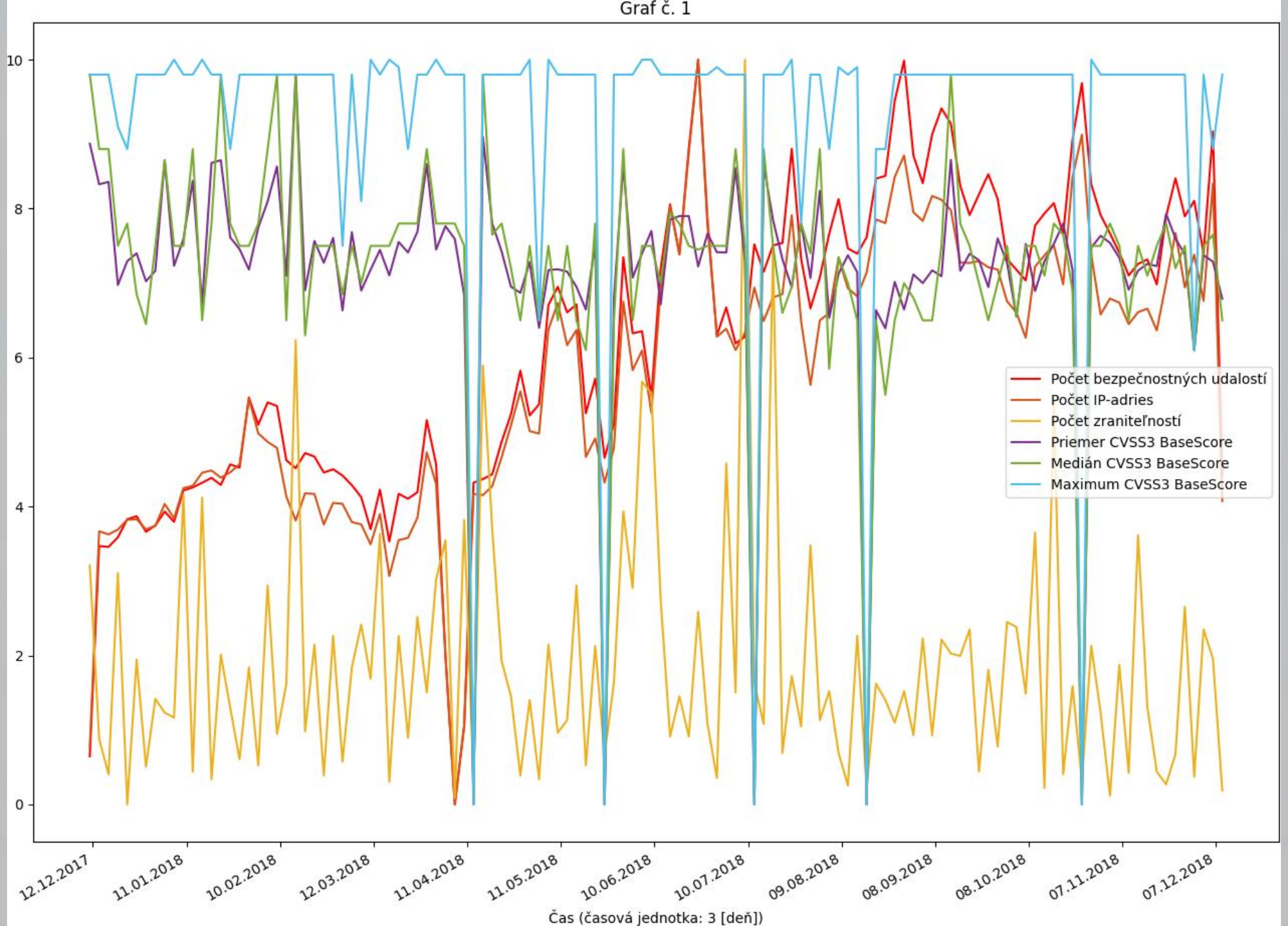
Zraniteľnosti

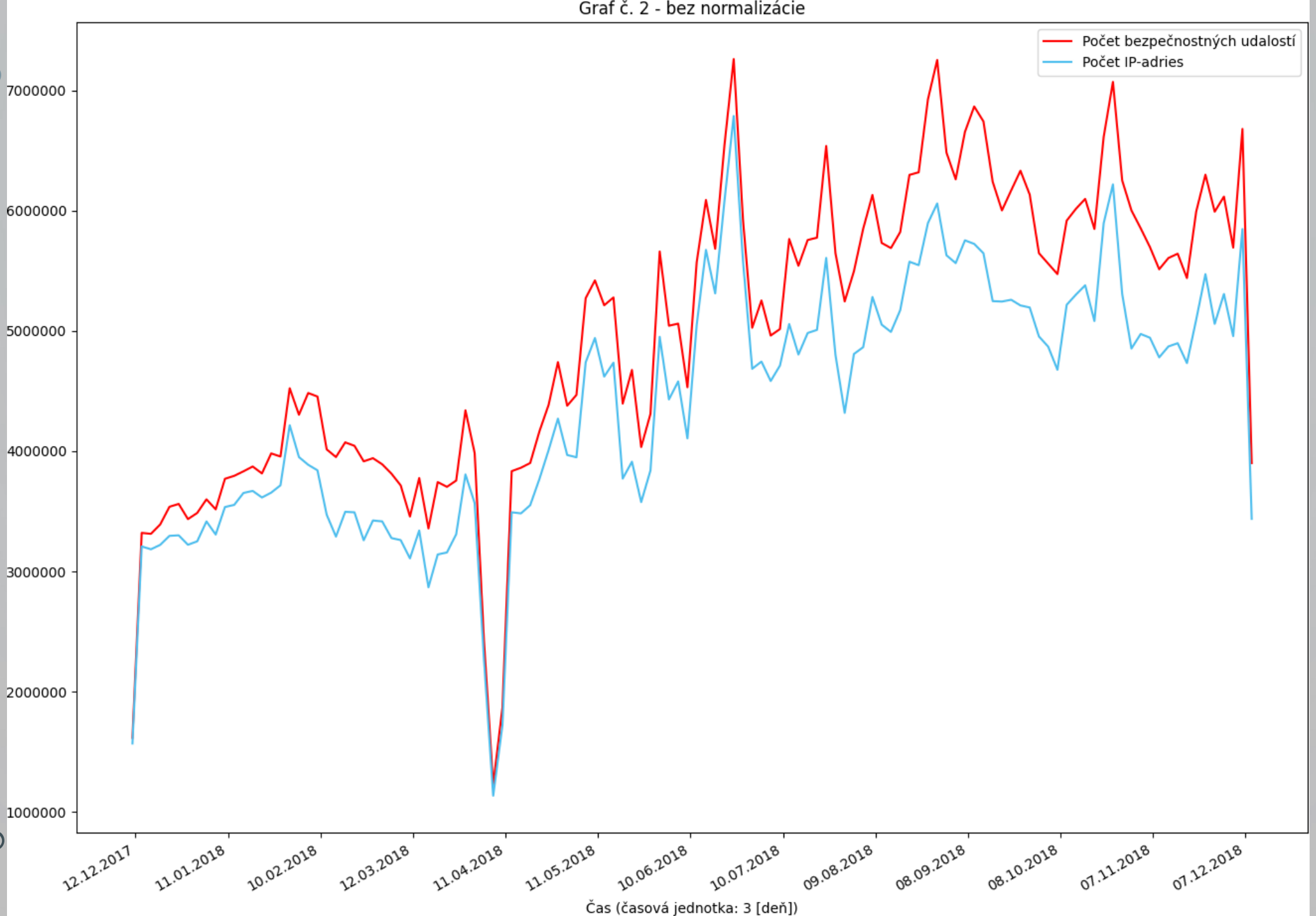
- pôvod – NVD NIST (nvd.nist.gov)
- 47 časových radov
- časový úsek – 1 rok

Atribút	Možné hodnoty
id	CVE-rok-číslo
publishedDate	-
lastModifiedDate	-
attackVector	network, adjacent_network, local, physical
attackComplexity	low, high
privilegesRequired	none, low, high
userInteraction	none, required
scope	unchanged, changed
confidentialityImpact	none, low, high
integrityImpact	none, low, high
availabilityImpact	none, low, high
baseSeverity	none, low, medium, high, critical
exploitabilityScore	none, low, medium, high, critical
impactScore	none, low, medium, high, critical
cvss2BaseScore	none, low, medium, high, critical
cvss3BaseScore	none, low, medium, high, critical
cweInfo	CWE-číslo
description	popis

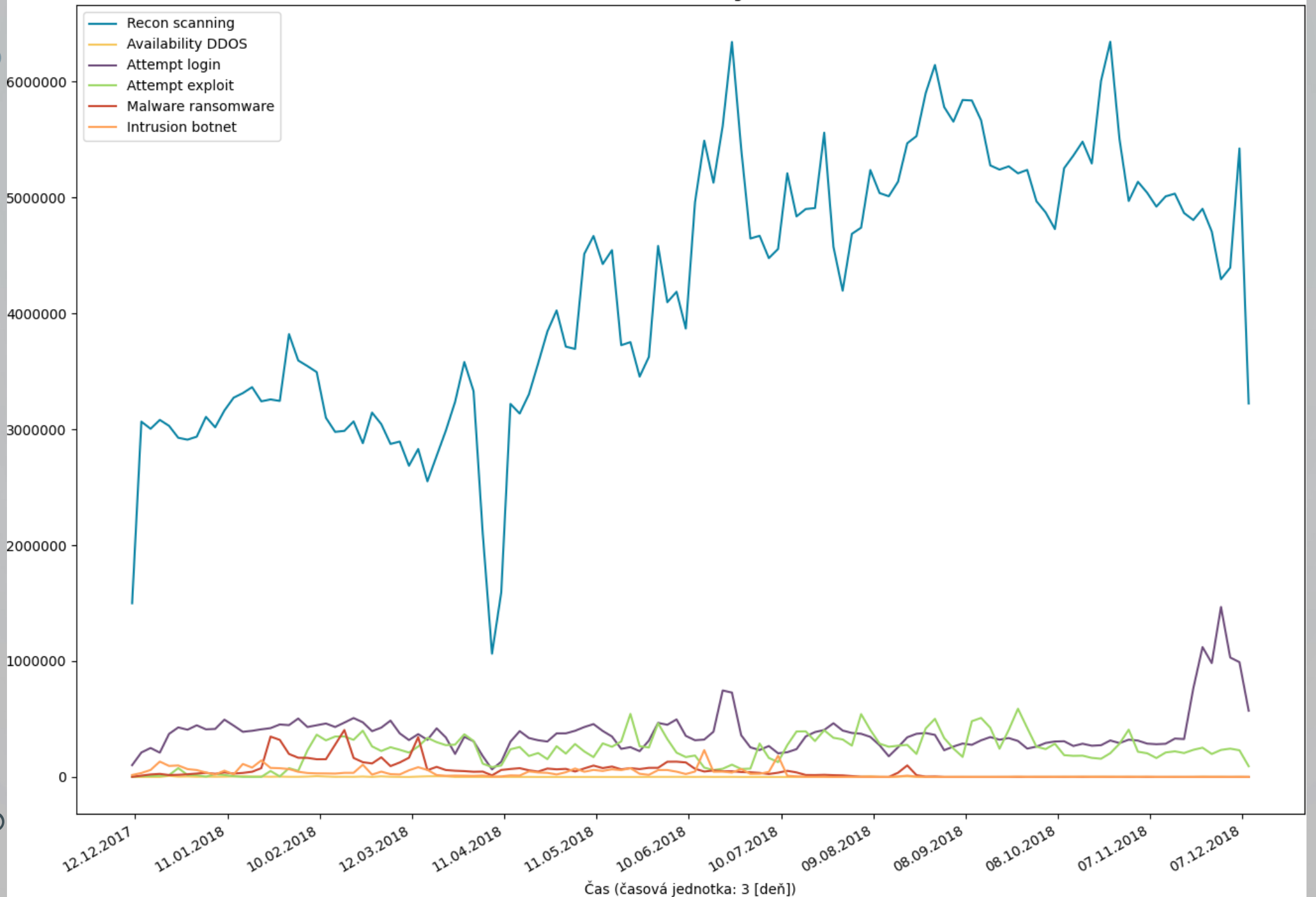
SPRACOVANIE DATASETOV

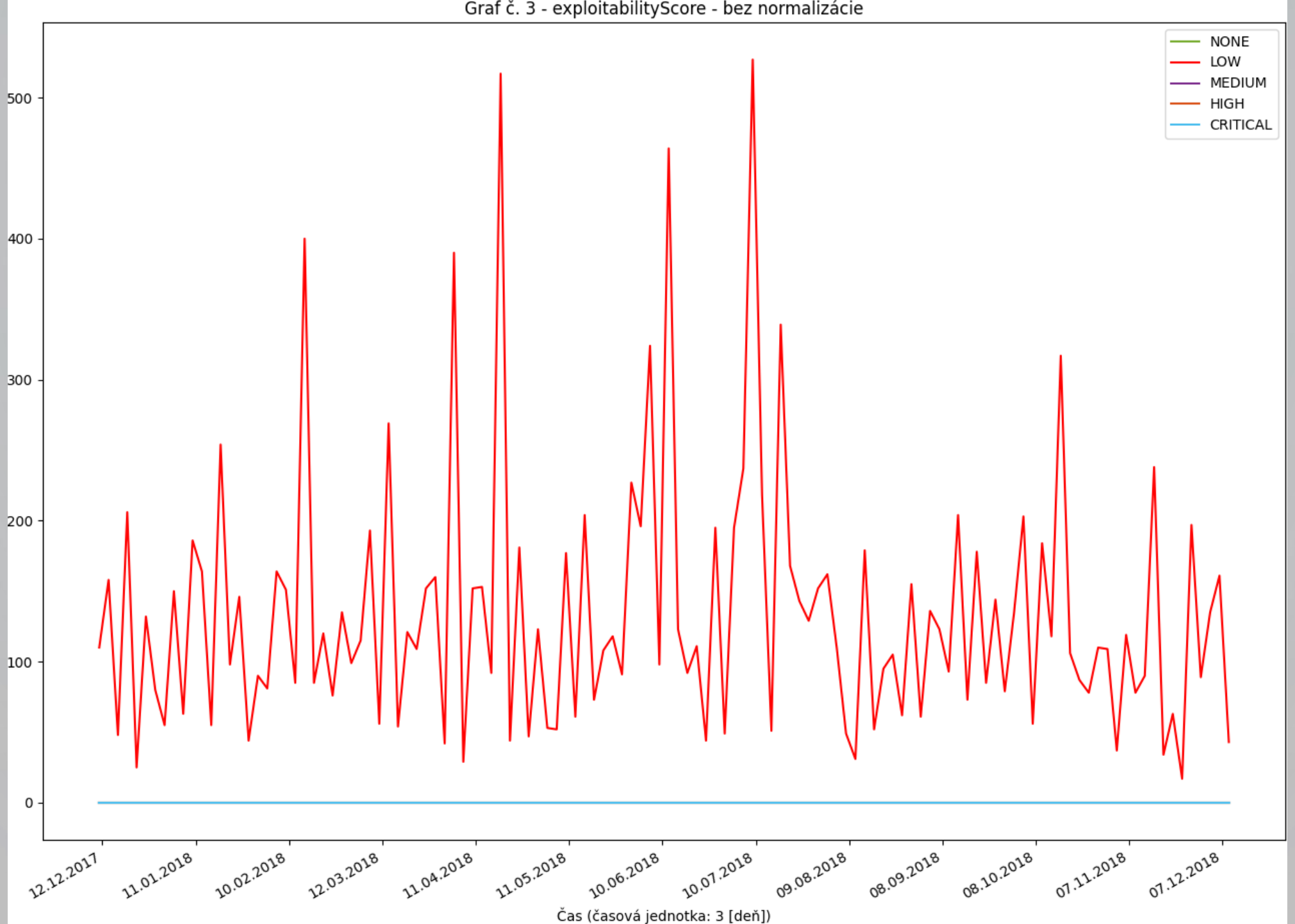
- vytvorenie časových radov (22 + 47 + doplnkové)
- nulové hodnoty
- výber vhodnej časovej jednotky
- základné prehľady
- korelácie


Graf č. 1
10
8
6
4
2
0
Počet bezpečnostných udalostí
Počet IP-adries
Počet zraniteľností
Priemer CVSS3 BaseScore
Medián CVSS3 BaseScore
Maximum CVSS3 BaseScore
12.12.2017
11.01.2018
10.02.2018
12.03.2018
11.04.2018
11.05.2018
10.06.2018
10.07.2018
09.08.2018
08.09.2018
08.10.2018
07.11.2018
07.12.2018
Čas (časová jednotka: 3 [deň])


Graf č. 2 - bez normalizácie
Počet bezpečnostných udalostí
Počet IP-adries
7000000
6000000
5000000
4000000
3000000
2000000
1000000
12.12.2017
11.01.2018
10.02.2018
12.03.2018
11.04.2018
11.05.2018
10.06.2018
10.07.2018
09.08.2018
08.09.2018
08.10.2018
07.11.2018
07.12.2018
Čas (časová jednotka: 3 [deň])

Graf. č. 4 - Kategórie

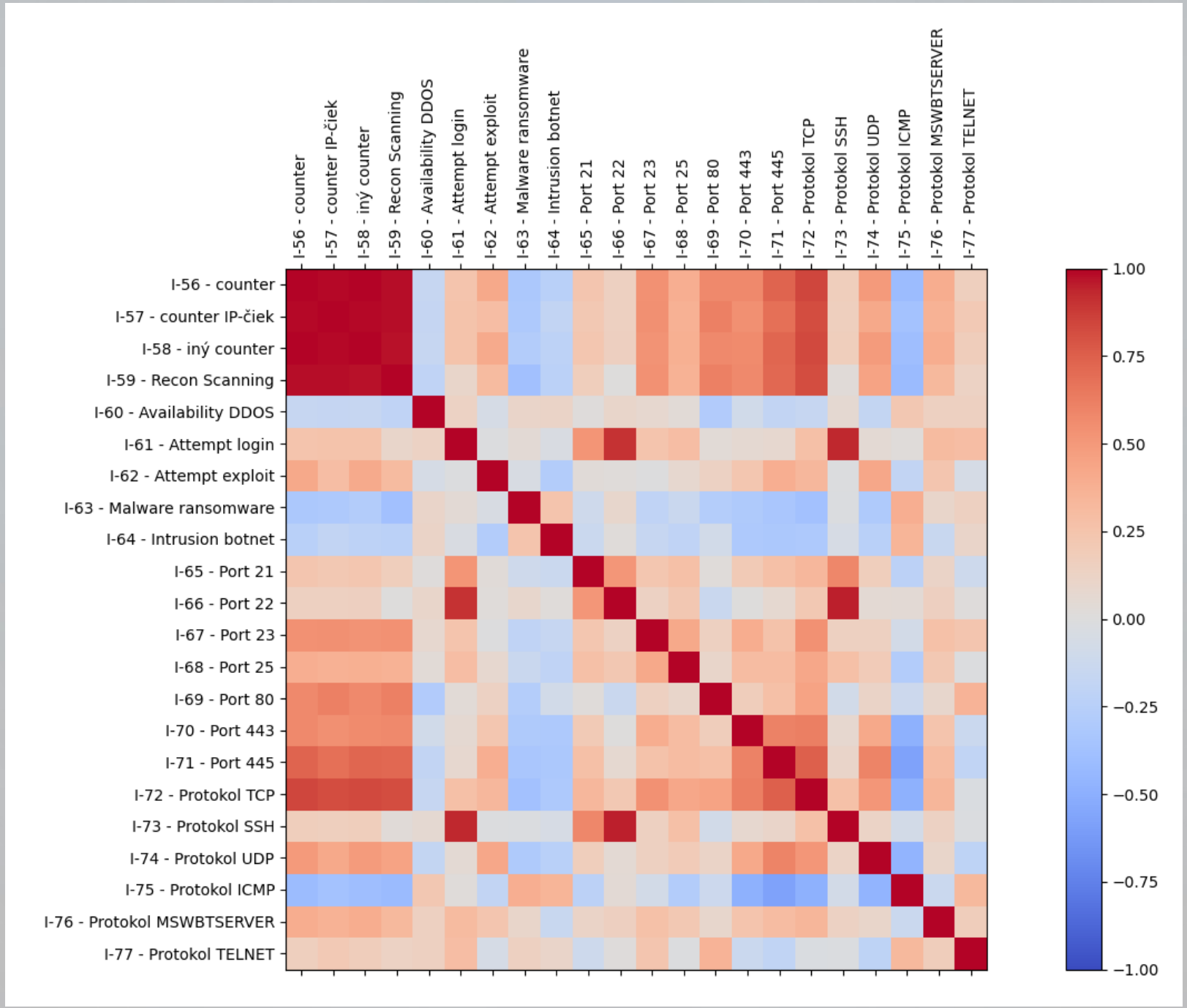



Graf č. 3 - exploitabilityScore - bez normalizácie
NONE
LOW
MEDIUM
HIGH
CRITICAL
500
400
300
200
100
0
12.12.2017
11.01.2018
10.02.2018
12.03.2018
11.04.2018
11.05.2018
10.06.2018
10.07.2018
09.08.2018
08.09.2018
08.10.2018
07.11.2018
07.12.2018
Čas (časová jednotka: 3 [deň])

Popis	1 deň	2 dni	3 dni
counter	0,27	0,55	0
counter IP-čiek	0,27	0,55	0
counter(iný ako 56)	0,27	0,55	0
recon scanning	0,27	0,55	0
availability DDOS	**9,32**	**5,46**	**3,28**
attempt login	0,27	0,55	0
attempt exploit	0,27	0,55	0
malware ransomware	**29,04**	**28,42**	**27,87**
intrusion botnet	0,55	0,55	0
port 21	0,27	0,55	0
port 22	0,27	0,55	0
port 23	0,27	0,55	0
port 25	0,27	0,55	0
port 80	0,27	0,55	0
port 443	0,27	0,55	0
port 445	0,27	0,55	0
protokol TCP	0,27	0,55	0
protokol SSH	0,27	0,55	0
protokol UDP	0,27	0,55	0
protokol ICMP	0,27	0,55	0
protokol MSWBTSERVER	0,27	0,55	0
protokol TELNET	0,27	0,55	0

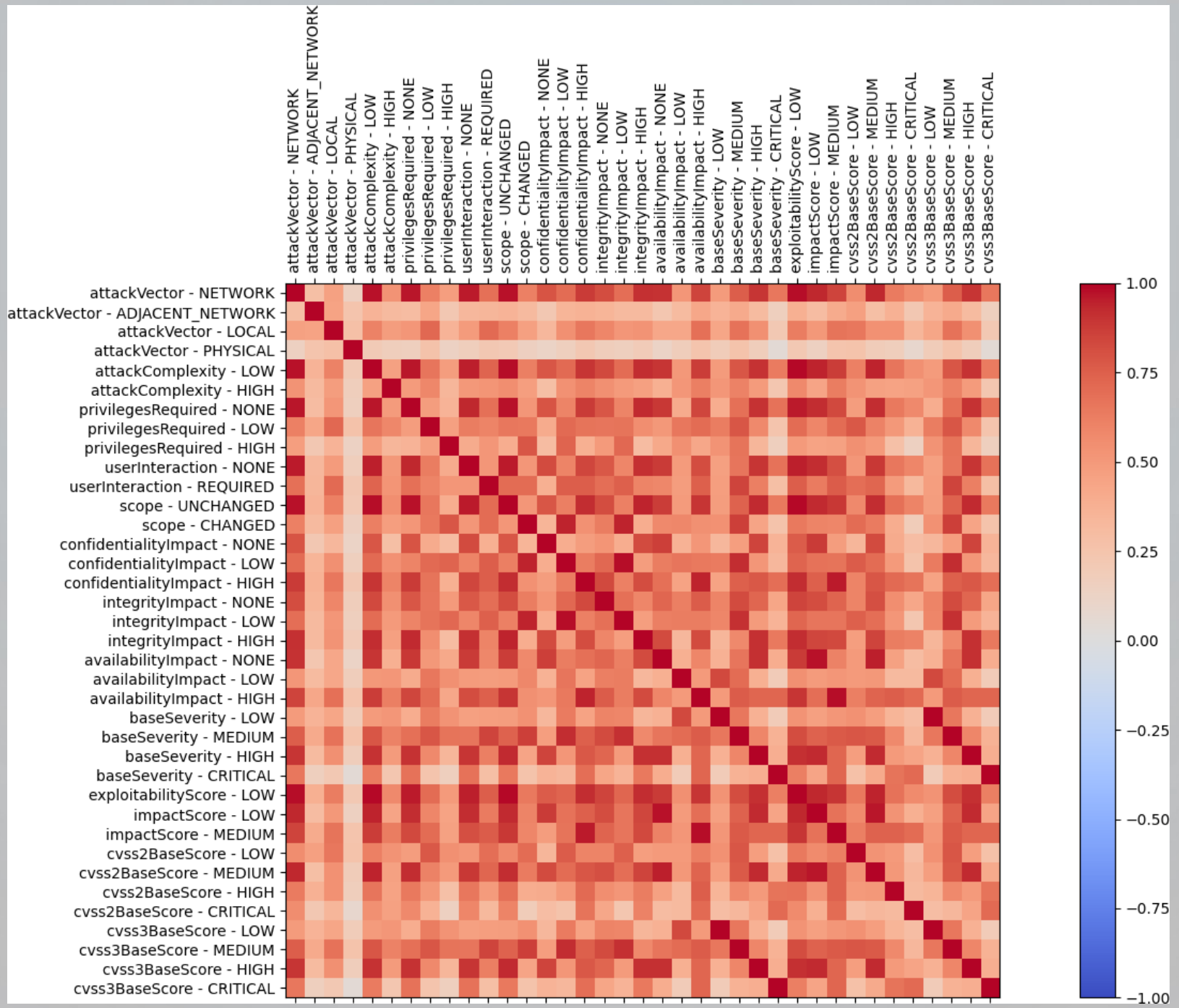
NULOVÉ HODNOTY - ZRANITEĽNOSTI

- base severity – none
- exploitability score – none, medium, high, critical
- impact score – none, high, critical
- cvss2 base score – none
- cvss3 base score – none


I-56 - counter
I-57 - counter IP-čiek
I-58 - iný counter
I-59 - Recon Scanning
I-60 - Availability DDOS
I-61 - Attempt login
I-62 - Attempt exploit
I-63 - Malware ransomware
I-64 - Intrusion botnet
I-65 - Port 21
I-66 - Port 22
I-67 - Port 23
I-68 - Port 25
I-69 - Port 80
I-70 - Port 443
I-71 - Port 445
I-72 - Protokol TCP
I-73 - Protokol SSH
I-74 - Protokol UDP
I-75 - Protokol ICMP
I-76 - Protokol MSWBTSERVER
I-77 - Protokol TELNET
1.00
0.75
0.50
0.25
0.00
−0.25
−0.50
−0.75
−1.00

KORELÁCIE - UDALOSTI

- recon scanning + TCP + port 80
- TCP + port 80
- TCP + port 22
- attempt login + SSH + port 22


attackVector - NETWORK
attackVector - ADJACENT_NETWORK
attackVector - LOCAL
attackVector - PHYSICAL
attackComplexity - LOW
attackComplexity - HIGH
privilegesRequired - NONE
privilegesRequired - LOW
privilegesRequired - HIGH
userInteraction - NONE
userInteraction - REQUIRED
scope - UNCHANGED
scope - CHANGED
confidentialityImpact - NONE
confidentialityImpact - LOW
confidentialityImpact - HIGH
integrityImpact - NONE
integrityImpact - LOW
integrityImpact - HIGH
availabilityImpact - NONE
availabilityImpact - LOW
availabilityImpact - HIGH
baseSeverity - LOW
baseSeverity - MEDIUM
baseSeverity - HIGH
baseSeverity - CRITICAL
exploitabilityScore - LOW
impactScore - LOW
impactScore - MEDIUM
cvss2BaseScore - LOW
cvss2BaseScore - MEDIUM
cvss2BaseScore - HIGH
cvss2BaseScore - CRITICAL
cvss3BaseScore - LOW
cvss3BaseScore - MEDIUM
cvss3BaseScore - HIGH
cvss3BaseScore - CRITICAL
1.00
0.75
0.50
0.25
0.00
−0.25
−0.50
−0.75
−1.00

	attackComplexity_HIGH	attackComplexity_LOW	attackVector_ADJACENT_NETWORK	attackVector_LOCAL	attackVector_NETWORK	attackVector_PHYSICAL	availabilityImpact_HIGH	availabilityImpact_LOW	availabilityImpact_NONE
attackComplexity_HIGH	-								
attackComplexity_LOW	0,48	-							
attackVector_ADJACENT_NETWORK	0,28	0,51	-						
attackVector_LOCAL	0,49	0,67	0,37	-					
attackVector_NETWORK	0,54	0,95	0,45	0,45	-				
attackVector_PHYSICAL	0,09	0,37	0,24	0,32	0,28	-			
availabilityImpact_HIGH	0,57	0,92	0,52	0,76	0,84	0,36	-		
availabilityImpact_LOW	0,46	0,42	0,18	0,25	0,46	0,11	0,31	-	
availabilityImpact_NONE	0,49	0,92	0,42	0,49	0,93	0,3	0,71	0,44	-
baseScore_CRITICAL	0,33	0,72	0,39	0,4	0,72	0,2	0,77	0,2	0,54
baseScore_HIGH	0,56	0,92	0,48	0,64	0,89	0,3	0,87	0,31	0,86
baseScore_MEDIUM	0,51	0,89	0,45	0,62	0,86	0,38	0,79	0,55	0,86
baseScore_LOW	0,32	0,5	0,24	0,48	0,44	0,24	0,38	0,61	0,52
baseScore_NONE	-	-	-	-	-	-	-	-	-
baseSeverity_CRITICAL	0,34	0,72	0,39	0,4	0,72	0,2	0,77	0,21	0,55
baseSeverity_HIGH	0,59	0,92	0,48	0,66	0,89	0,3	0,88	0,31	0,86
baseSeverity_MEDIUM	0,51	0,89	0,45	0,62	0,86	0,38	0,78	0,55	0,86

KORELÁCIE - ZRANITEĽNOSTI

- attack complexity LOW – privileges required NONE
- attack complexity LOW – scope UNCHANGED
- impact score MEDIUM – confidentiality impact HIGH
- impact score MEDIUM – availability impact HIGH
- ...

UDALOSTI - ZRANITEĽNOSTI

- vzťah?

UDALOSTI - ZRANITEĽNOSTI

- vzťah?
- zraniteľnosti ➡ udalosti
- aké sú vzťahy medzi radmi udalostí?
- aké rady zraniteľností ovplyvňujú udalosti?

VECTOR AUTORREGRESSION (VAR)

- tento model pracuje s predchádzajúcimi hodnotami
- TS/premenná je modelovaná pomocou seba a ostatných
- obojsmerné vzťahy

$$Y_{1,t} = \alpha_1 + \beta_{11,1} Y_{1,t-1} + \beta_{12,1} Y_{2,t-1} + \epsilon_{1,t}$$
$$Y_{2,t} = \alpha_2 + \beta_{21,1} Y_{1,t-1} + \beta_{22,1} Y_{2,t-1} + \epsilon_{2,t}$$

$$Y_{1,t} = \alpha_1 + \beta_{11,1} Y_{1,t-1} + \beta_{12,1} Y_{2,t-1} + \beta_{11,2} Y_{1,t-2} + \beta_{12,2} Y_{2,t-2} + \epsilon_{1,t}$$
$$Y_{2,t} = \alpha_2 + \beta_{21,1} Y_{1,t-1} + \beta_{22,1} Y_{2,t-1} + \beta_{21,2} Y_{1,t-2} + \beta_{22,2} Y_{2,t-2} + \epsilon_{2,t}$$

GRANGER´S CAUSALITY TEST

- otestovanie, či sú vzájomné vzťahy medzi TS
- nulová hypotéza – X neovyplvňuje Y ($p > 0.05$)

	rgnp_x	pgnp_x	ulc_x
rgnp_y	1.0000	0.0003	0.0001
pgnp_y	0.0000	1.0000	0.0000
ulc_y	0.0000	0.0000	1.0000

GRANGER´S CAUSALITY TEST

- events(count) – availability impact NONE
  – confidentiality impact HIGH
  – integrity impact HIGH
  – impact score MEDIUM
  – cvss2 base score CRITICAL
- attempt login, port 22, SSH

COINTEGRATION AND STATIONARITY TEST

- cointegration – zisťujeme štatisticky významný vzťah medzi TS
  – či lin. kombináciu TS stačí menejkrát diferencovať ako jednotlivé TS
- stationarity – bez trendu a sezónnosti, z dlhodobého hľadiska žiaden predvídateľný vzor

VÝBER P PRE VAR(P)

VAR Order Selection (* highlights the minimums)

	AIC	BIC	FPE	HQIC
0	35.15	35.20	1.835e+15	35.17
1	34.62	34.79	1.086e+15	34.69
2	34.36	34.65*	8.348e+14	34.47*
3	34.42	34.83	8.918e+14	34.59
4	34.34	34.86	8.215e+14	34.55
5	34.37	35.00	8.486e+14	34.63
6	34.24	34.99	7.472e+14	34.54
7	34.28	35.14	7.767e+14	34.63
8	34.20	35.18	7.192e+14*	34.59
9	34.25	35.34	7.626e+14	34.69
10	34.34	35.55	8.370e+14	34.83
11	34.31	35.64	8.204e+14	34.84
12	34.19*	35.62	7.283e+14	34.76

TRÉNOVANIE

- dostaneme základné informácie o modeli, koeficienty rovníc jednotlivé časové rady

```
Results for equation impactScore-MEDIUM
=======================================
                            coefficient
---------------------------------------
const                         -1.226639
L1.events                     -0.000014
L1.impactScore-MEDIUM         -0.921527
L2.events                      0.000022
L2.impactScore-MEDIUM         -0.394878
=======================================
```

SERIAL CORRELATION OF RESIDUALS (DURBIN WATSON STATISTICS)

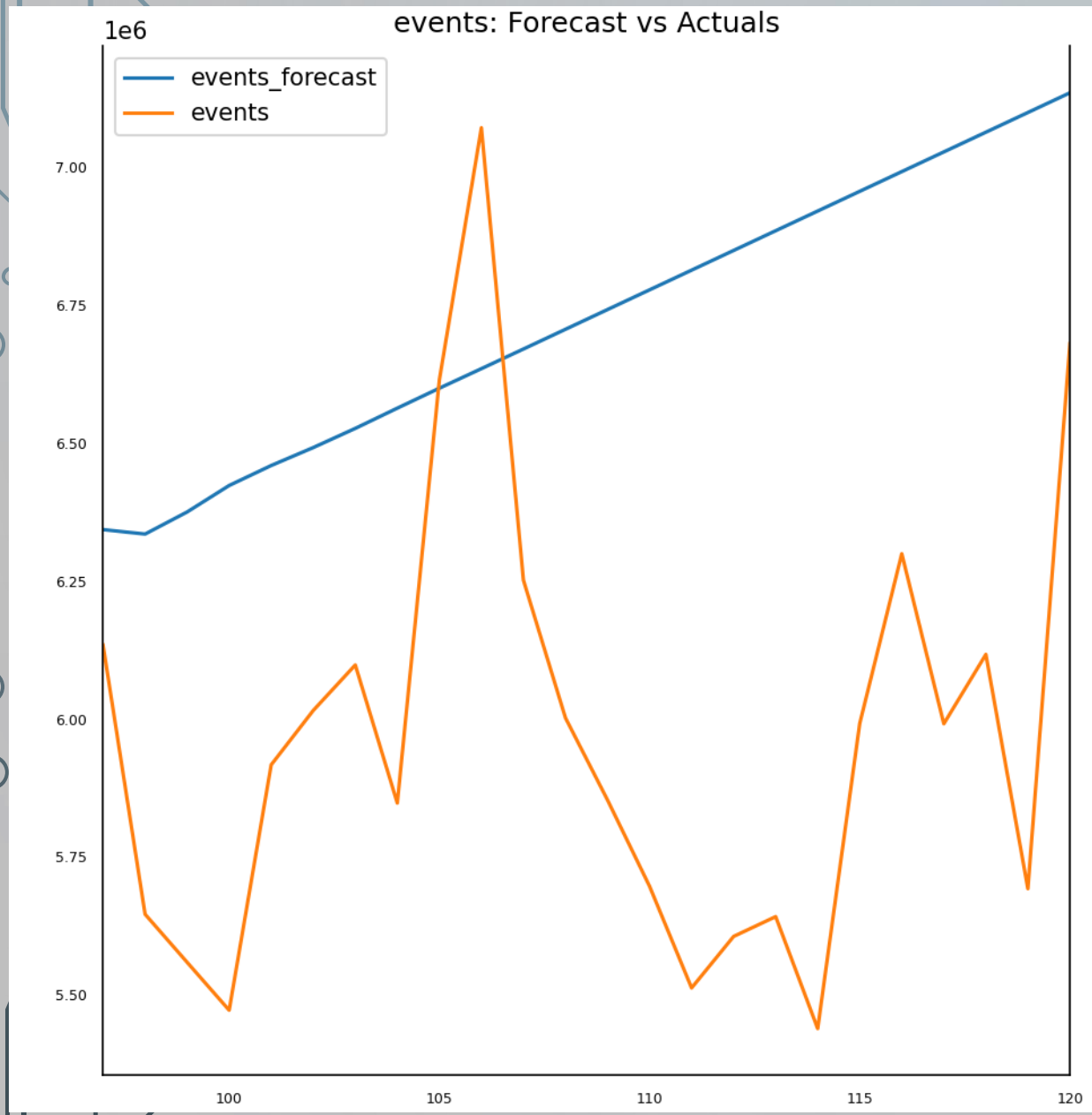
- na odhalenie prípadného vzoru v chybách, ktorý by bolo potrebné vysvetliť modelom
- hodnoty od 0 po 4:
  - blízko 0 – kladná korelácia
  - blízko 2 – bez významnej korelácie
  - blízko 4 – záporná korelácia

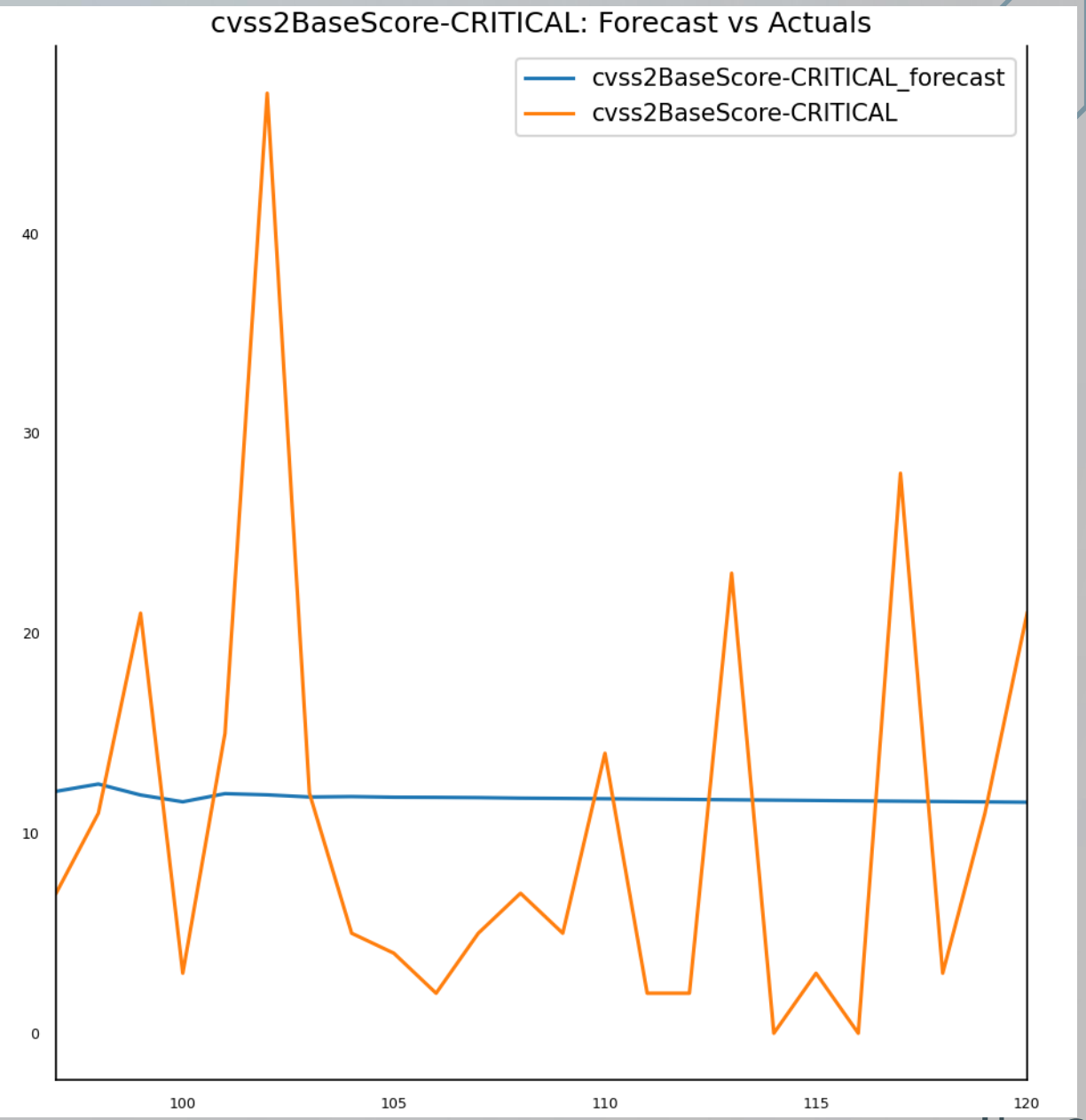
$$DW = \frac{\Sigma_{t=2}^{T}((e_t - e_{t-1})^2)}{\Sigma_{t=1}^{T} e_t^2}$$

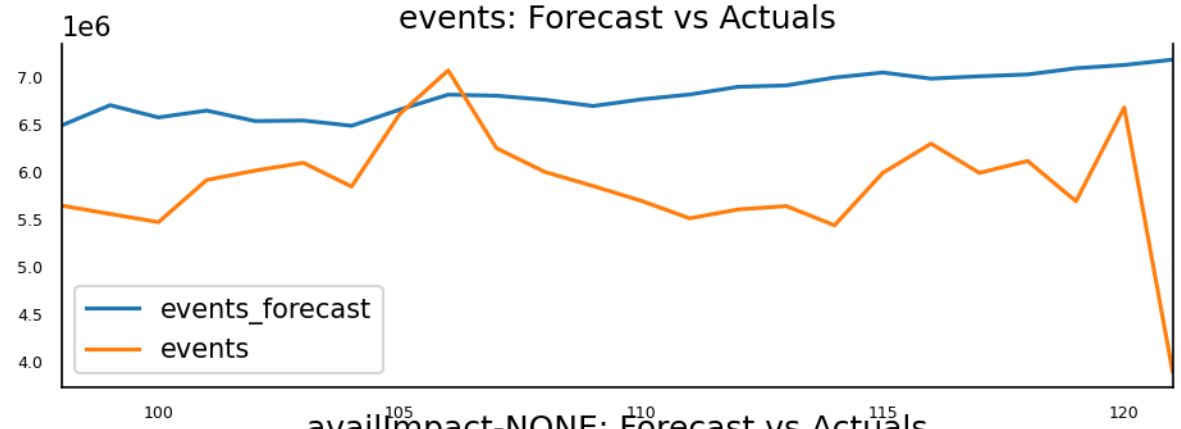
```
events : 2.03
impactScore-MEDIUM : 2.02
```

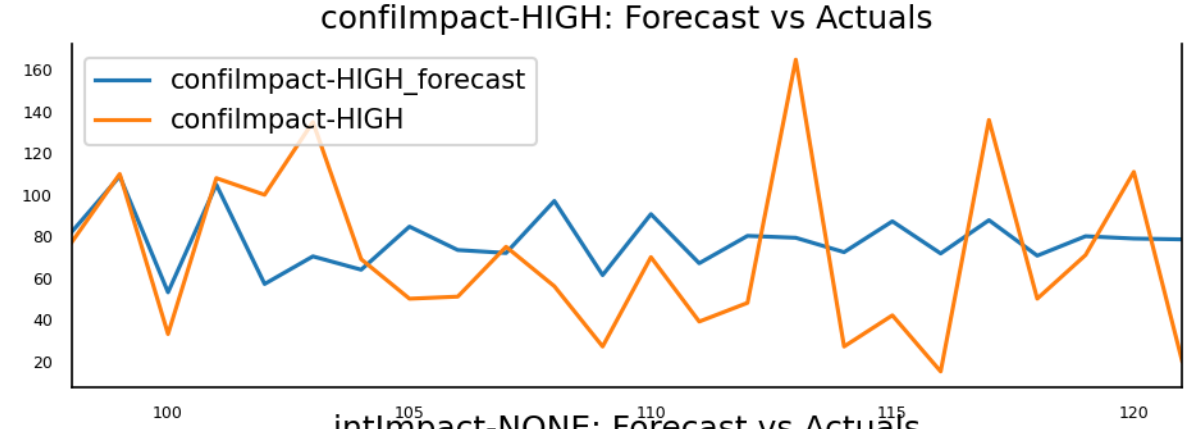
PREDIKCIA

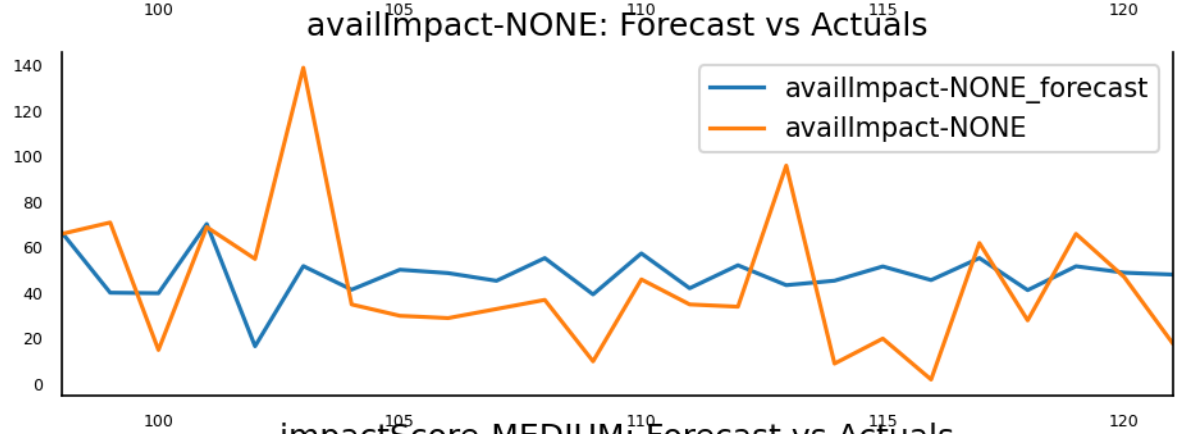
- predikcia
- transformovanie hodnôt (ak bolo potrebné diferencovanie)
- vizualizácia
- vyhodnotenie(MAPE, ME, MAE, MPE, RMSE)

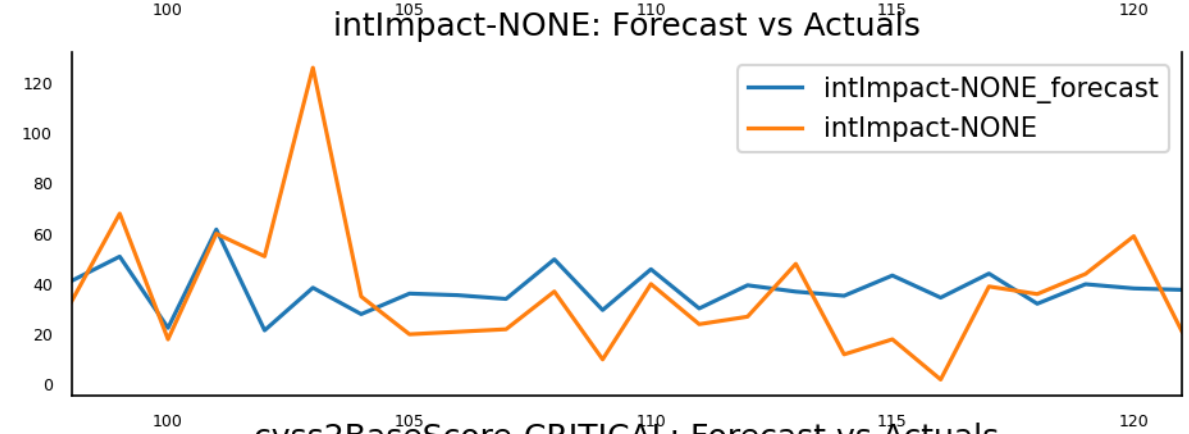

events: Forecast vs Actuals
1e6
events_forecast
events
7.00
6.75
6.50
6.25
6.00
5.75
5.50
100
105
110
115
120

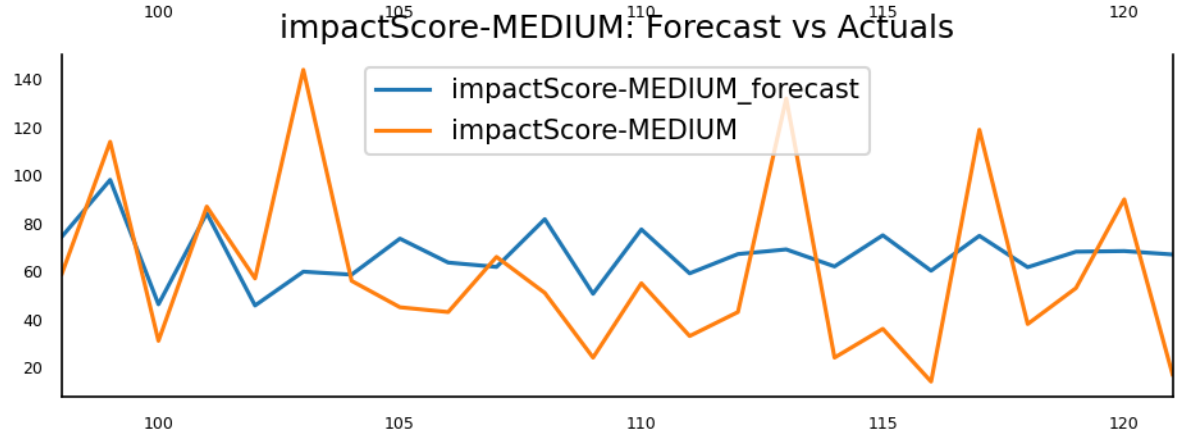

cvss2BaseScore-CRITICAL: Forecast vs Actuals
cvss2BaseScore-CRITICAL_forecast
cvss2BaseScore-CRITICAL
40
30
20
10
0
100
105
110
115
120

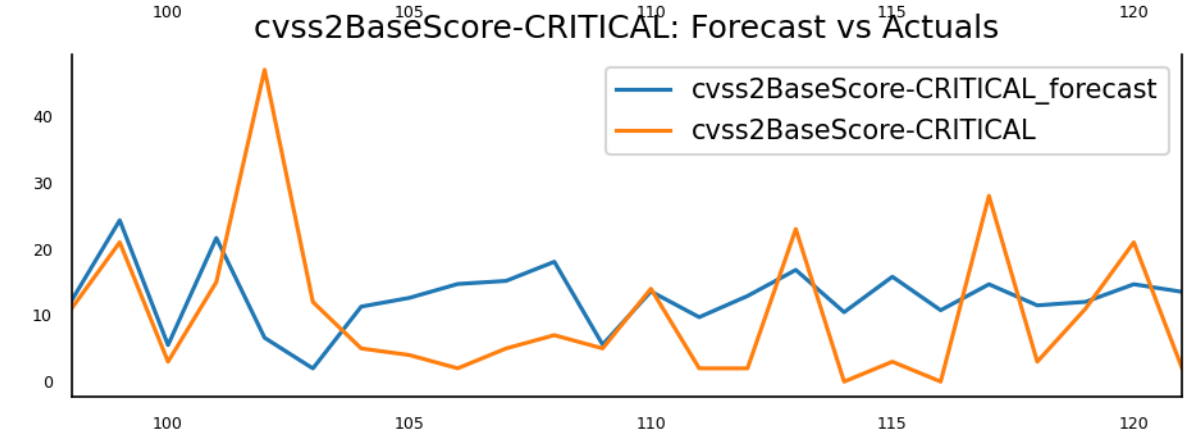

events: Forecast vs Actuals
1e6
events_forecast
events

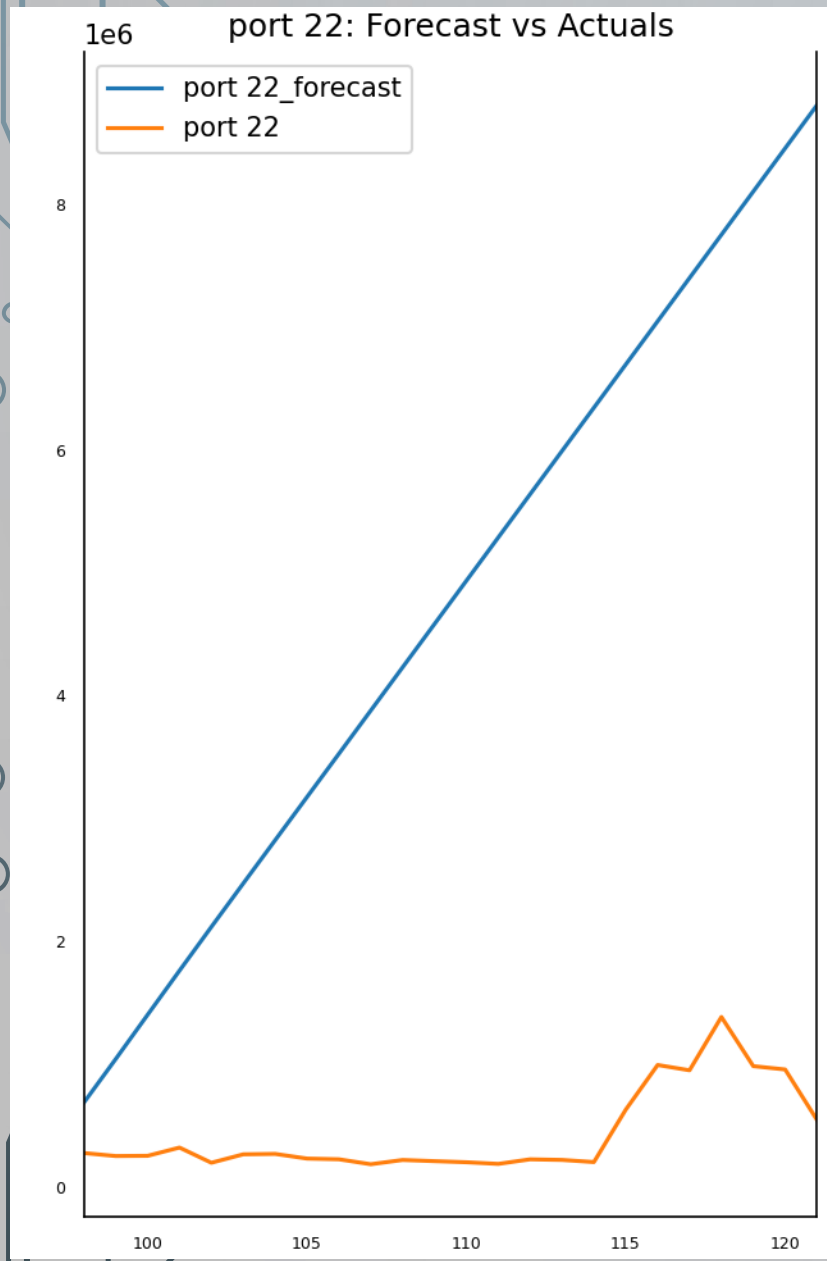

confiImpact-HIGH: Forecast vs Actuals
confiImpact-HIGH_forecast
confiImpact-HIGH

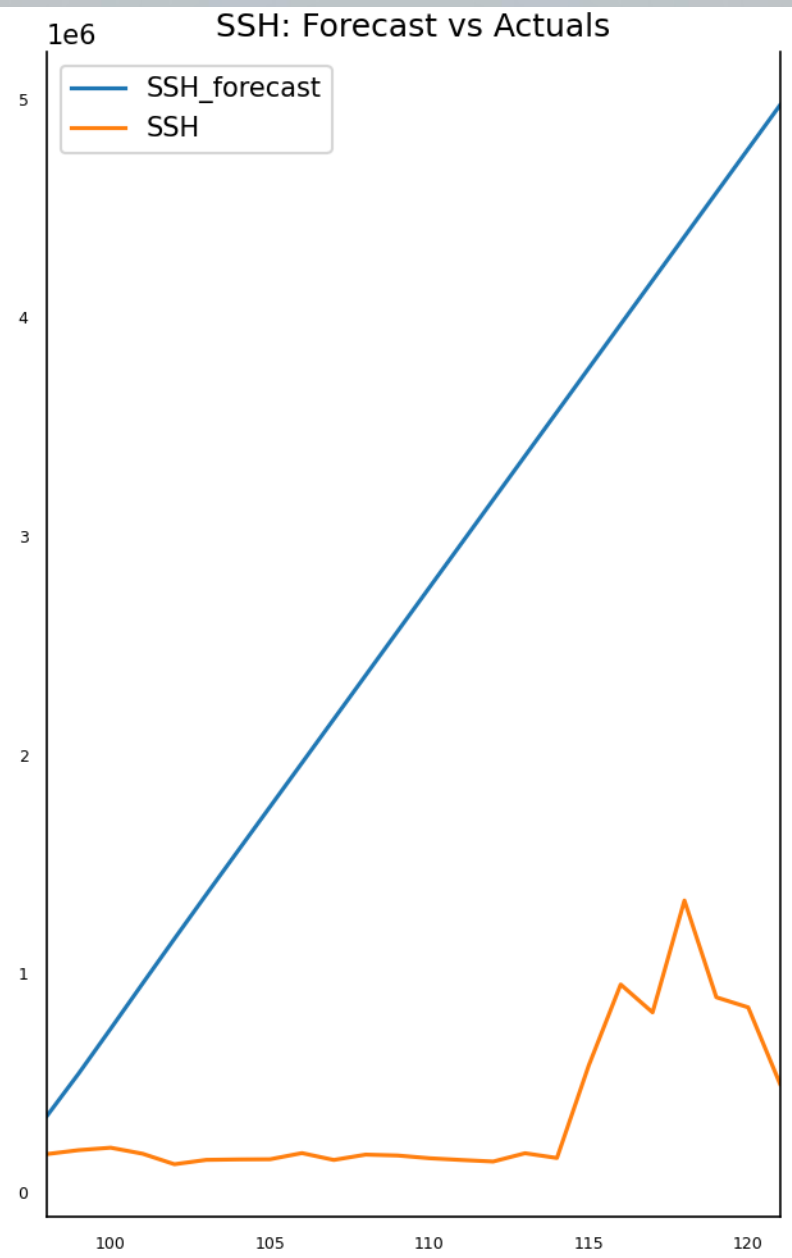

availImpact-NONE: Forecast vs Actuals
availImpact-NONE_forecast
availImpact-NONE

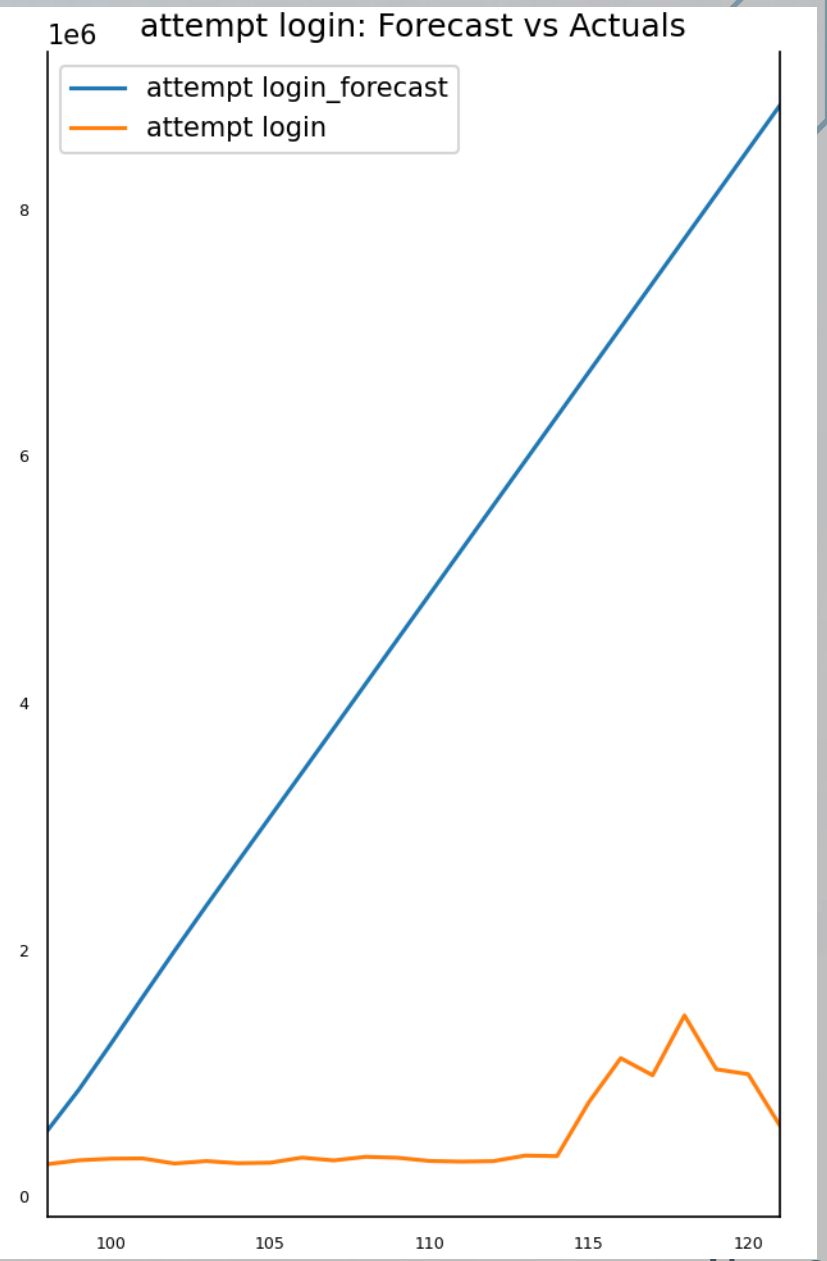

intImpact-NONE: Forecast vs Actuals
intImpact-NONE_forecast
intImpact-NONE


impactScore-MEDIUM: Forecast vs Actuals
impactScore-MEDIUM_forecast
impactScore-MEDIUM


cvss2BaseScore-CRITICAL: Forecast vs Actuals
cvss2BaseScore-CRITICAL_forecast
cvss2BaseScore-CRITICAL


port 22: Forecast vs Actuals
1e6
port 22_forecast
port 22
8
6
4
2
0
100
105
110
115
120


SSH: Forecast vs Actuals
1e6
SSH_forecast
SSH
5
4
3
2
1
0
100
105
110
115
120


attempt login: Forecast vs Actuals
1e6
attempt login_forecast
attempt login
8
6
4
2
0
100
105
110
115
120

LITERATÚRA

- Hyndman, R.J., & Athanasopoulos, G. (2021) Forecasting: principles and practice, 3rd edition, OTexts: Melbourne, Australia. OTexts.com/fpp3. Accessed on 15. 12. 2021.
- Vector Autoregression (VAR) - Comprehensive Guide with Examples in Python - Machine Learning Plus, https://www.machinelearningplus.com/time-series/vector-autoregression-examples-python/, accesed on 15. 12. 2021.

ĎAKUJEM ZA POZORNOSŤ

☺